August 2, 2012
Version 1.1

NOAA Rules of Behavior for Mobile Devices

The purpose of this document is to the outline the conditions that NOAA requires to allow a smartphone, tablet computer or any other portable electronic device, but not including laptops or desktops ("Mobile Device") to connect to NOAA IT systems, including connecting to the NOAA email system. By signing this document, the user agrees to abide by the NOAA IT Rules of Behavior, all other Department of Commerce and NOAA and Line Office IT Security Policies which are found at www.cio.noaa.gov/Policy_Programs/ciopol.html policies.

In addition, the following will apply to any Mobile Devices configured to connect to NOAA systems, including connecting to the NOAA email system. Specifically:

- NOAA and /or Line Office will install a set of configurations and controls known as an "IT Security Profile" on all Government-owned Mobile Devices.
- Non-Government owned Mobile Devices that connect to the NOAA Unified Message System (UMS or email) solely by means of a web browser through the Google Web interface, and do not otherwise store NOAA data on the Mobile Device outside the browser cache, do not require installation of an IT Security Profile. Mobile Devices that connect to any other NOAA system (or connect to the UMS by any other means) must have an IT Security Profile installed prior to doing so.
- The IT Security Profile may make some applications and Mobile Device features unusable. NOAA and or Line Offices will not provide support for any disabled applications or features and will not be responsible for any costs associated with the loss of such applications or features.
- Mobile Devices that lack a NOAA IT Security Profile or are not otherwise configured or managed by NOAA and/or a Line Office may only access UMS data (email, calendar, contacts, and NOAA Google Documents) through a web browser using the Google Web interface. (Note: IMAP/POP connection to UMS data to a personal device is not allowed).
- NOAA and/or a Line Office may require the installation of additional security and management related software as a condition of connecting a Mobile Device to any NOAA systems, other than a connecting to the UMS solely through a browser via the Google Web interface.
- In the event that an unauthorized change to a NOAA IT Security Profile, NOAA device configuration(s), or NOAA-required security control(s) is discovered on any device issued by NOAA or configured and managed by NOAA on behalf of a user, NOAA and/or a Line Office shall take immediate corrective action. Such corrective action can include, but is not limited to, selective erasing (removal of Government data and applications) of the contents of the device, by remotely wiping, denying the device access to NOAA systems, or restricting user access to NOAA systems. The selective remote wipe may be done at any time, without notice to the user. NOAA and /or Line Office will not be liable for any loss of data or applications resulting from a remote wipe.
- The user understands and agrees that if any NOAA data is stored on any Mobile Device outside of a browser cache, the device may be accessed, searched and reviewed pursuant to government investigations and /or litigation. The user further understands that he/she may lose access to or use of the Mobile Device during this review or search. The

user hereby agrees that NOAA and its Line Offices are not responsible for any cost, consequence (including any limitation of function or impairment of use), and/or loss resulting from any mandated review or corrective action.

- NOAA IT Offices will not provide support for or be responsible for costs associated with non-work related applications on any Mobile Device.
- Non-government data may not be retained, downloaded, or copied from the Mobile Device to a government computer or system, unless specifically authorized in the system security plan.
- Without specific authorization from a NOAA or Line Office IT security officer or designee, Mobile Devices, even Mobile Devices configured and managed by NOAA and/ or a Line Office, may not be physically connected to NOAA systems or computers. This includes the use of USB cables connected to a NOAA computer, even if the sole purpose is to charge the Mobile Device.
- Prior to taking a NOAA managed Mobile Device outside of the United States, for either business or personal travel, the user must notify the Line Office IT Security Officer or individual designated by the Line Office of:
    - Dates of travel
    - Countries of travel including stopovers and layovers
    - Identify any sensitive data that will be on the Mobile Device during travel
    - Comply with organizationally defined practices including maintaining possession of the device at all times, disabling WiFi and Bluetooth services, and such other controls as the Department of Commerce Office of Security (OSY), NOAA, or Line Office may impose
    - The user understands that the Mobile Device may need to be wiped (full device wipe to factory delivered state) upon return to the United States, prior to connection with any NOAA systems.

As Mobile Devices and operating systems continue to proliferate and change, NOAA and / or a Line Office cannot guarantee that any specific device, operating system or application version will work or continue to be supported.

User Acknowledgement and Acceptance

I certify by my signature below that I have read and to the best of my ability understand this document and agree to comply with its contents. I understand that my failure to comply may result in NOAA taking immediate corrective action(s) without prior notification, including the immediate wiping or disabling of any Mobile Device issued to me or configured and managed by NOAA on my behalf. I also understand and agree that personal data and applications on the Mobile Device may be lost as a result of NOAA's actions.

_____ _____

User Date